TISS
CYBERSECURITY
INSIGHTS

Annual Market Insights Report

2023

TRILLIUM
INFORMATION SECURITY SYSTEMS

www.trilliuminfosec.com

Table of Contents

Introduction

This report aims to uncover and understand the trends, insights, and challenges that organizations and cybersecurity professionals face in Pakistan. It addresses the critical gap in Pakistan-specific data within global security surveys. By providing localized insights and data, our goal is to offer valuable information tailored to the cybersecurity landscape in Pakistan. As pioneers of Information Security in Pakistan, we have been conducting a Market Insight Survey since 2016 to address the lack of industry-specific data related to cybersecurity.

To compile this report, we conducted a comprehensive survey involving over **100 organizations** in Pakistan, primarily from the enterprise sector. Our primary objective was to gain deep insights into the challenges and threats these organizations faced throughout the year to better comprehend the Cyber Threat Landscape of Pakistan and generate actionable Market Intelligence that organizations can use to appraise themselves and make well-calculated decisions. Utilizing Gartner Adaptive Security Architecture*, we sought to pinpoint the specific technologies essential for bolstering their cybersecurity programs and strategies. By providing Pakistan-specific data, our aim is to empower cybersecurity professionals and organizations in Pakistan to strategize and plan more effectively to address the unique challenges they encounter in the evolving cybersecurity landscape.

info@trilliuminfosec.com

www.trilliuminfosec.com

*https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization

Report Highlights

The survey results for this year have highlighted **Key Finding** that we believe are crucial for organizations to be aware of:

49% of organizations witnessed a notable increase of more than **10%** in their Information Security budget

45% of organizations have opted to outsource certain aspects of their cybersecurity operations

Phishing was responsible for more than **60%** of reported security incidents.

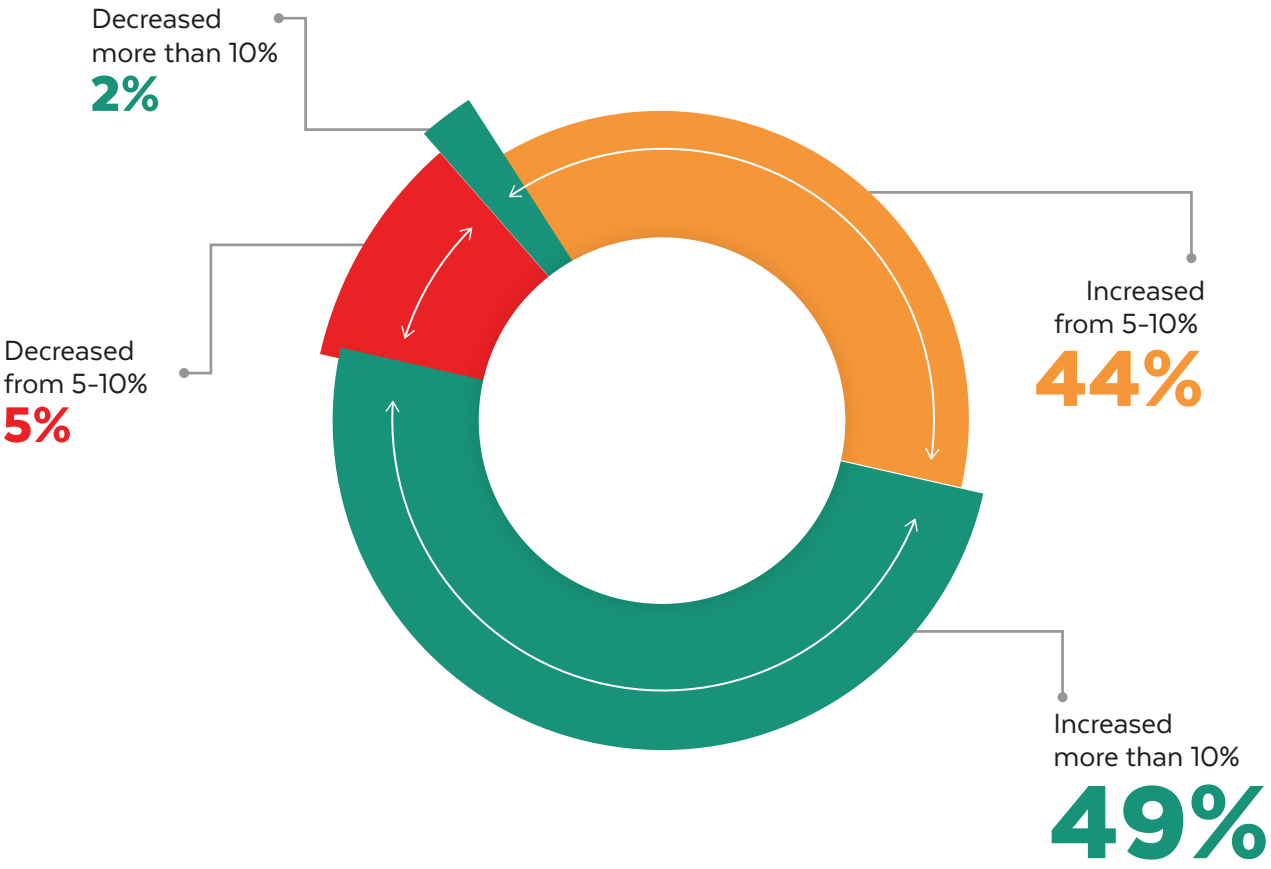
64% of organizations attributed their security challenges to a lack of Information Security awareness.

The most in-demand Prevention Technology is **Endpoint Security**

The most in-demand Detection Technology is **Security Information and Event Management (SIEM)**

The most in-demand Response Technology is **Forensics Tools**

Can you desribe the change in your year to year spending in terms of your information security budget?

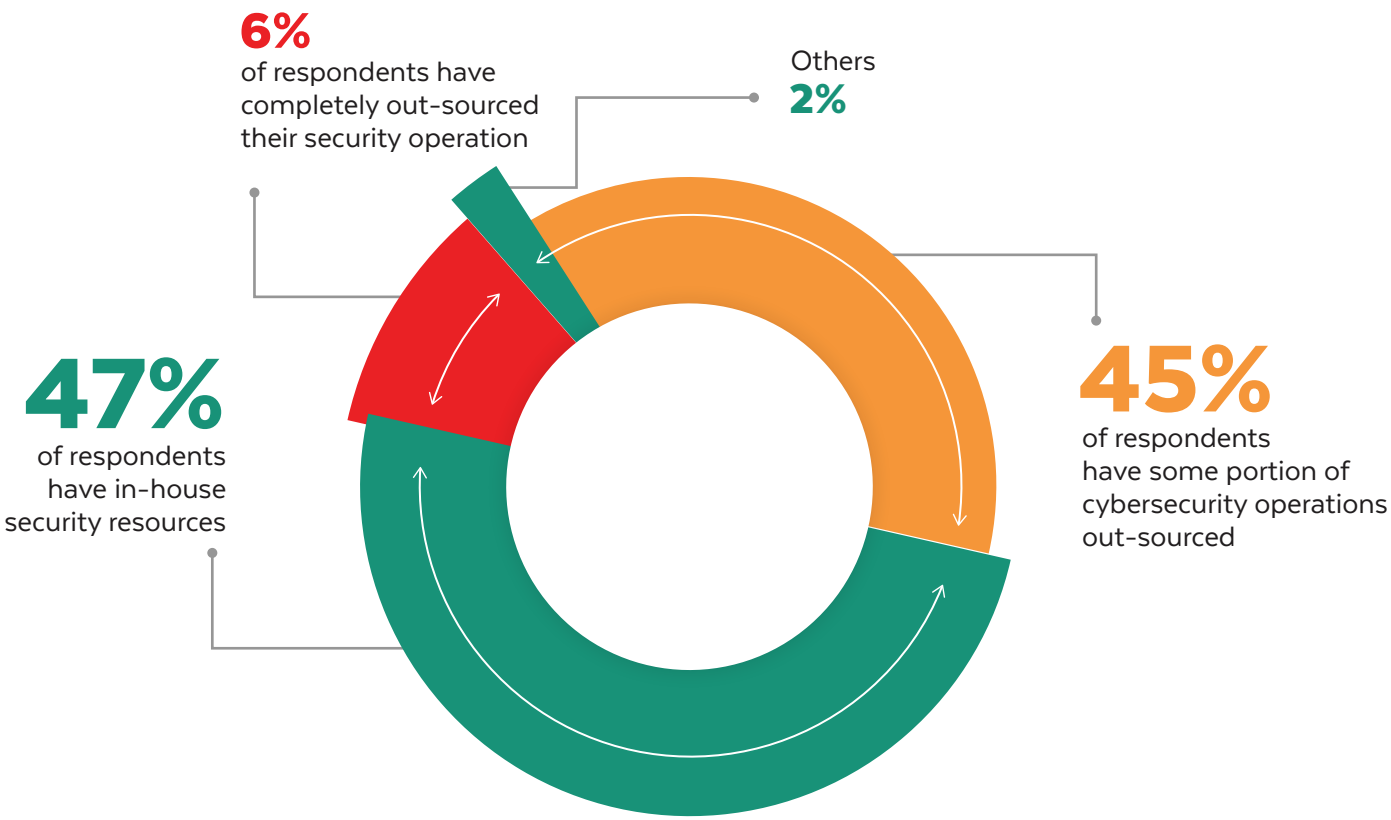


Key Takeaways

In terms of the year-to-year spending on information security budgets for the For the year 2023, the survey results indicate the following trends:

- A significant majority of respondents, 49% respondents reported a more substantial increase of over 10% in their information security budget for the same period.
- Additionally, 44% respondents, reported an increase in their information security budget ranging from 5% to 10% compared to the previous year.
- On the other hand, a small number of respondents, specifically 5% , mentioned a decrease in their information security budget within the range of 5% to 10% compared to the previous year.
- An even smaller number, consisting of 2% respondents, reported a more significant decrease of over 10% in their information security budget.

How are your security resources sourced?

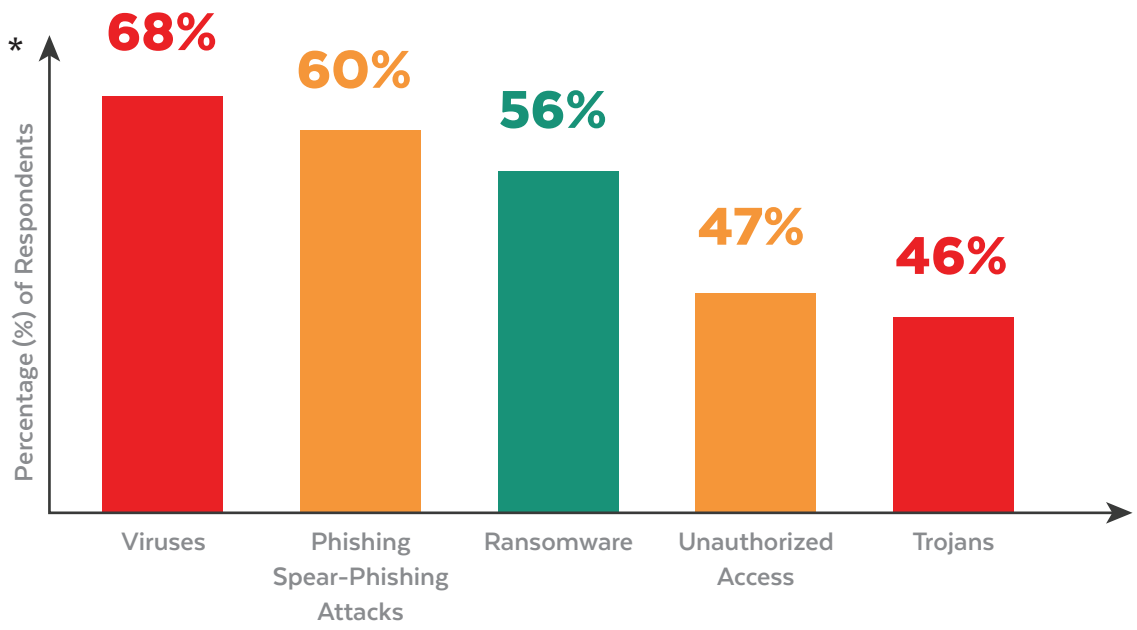


Key Takeaways

Organizations employ a range of strategies to source their security resources. Based on the survey results:

- Only 6% of respondents completely outsource their security resources and rely on external vendors or service providers.
- 47% of respondents rely on in-house resources, utilizing dedicated employees or teams for their security needs.
- 45% of respondents take a hybrid approach, combining in-house and outsourced resources to meet their security demands.
- 2% of respondents chose the options of Other, although specific details were not provided.

What were the top 5 cyber threats targeting your organization?

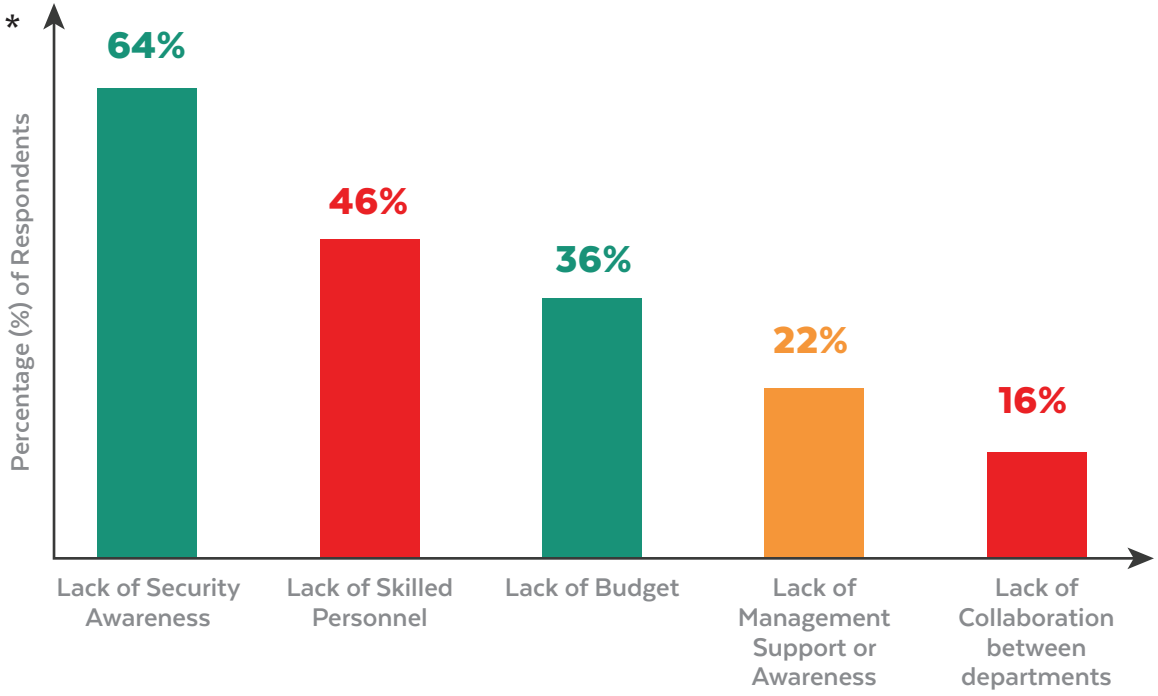


Key Takeaways

During the year, the top five cyber threats reported by organizations were viruses, ransomware, phishing/spear-phishing attacks, unauthorized access, and Trojans. These threats reflect the prevalence of malicious software, the ongoing risk of ransomware attacks, the persistence of social engineering tactics, the need for strong access control measures, and the deceptive nature of Trojans. These findings highlight the importance of implementing comprehensive cybersecurity measures to mitigate these threats effectively.

*Participants were allowed to select multiple options

Which of the following barriers inhibit your organization from adequately defending against cyber threats?



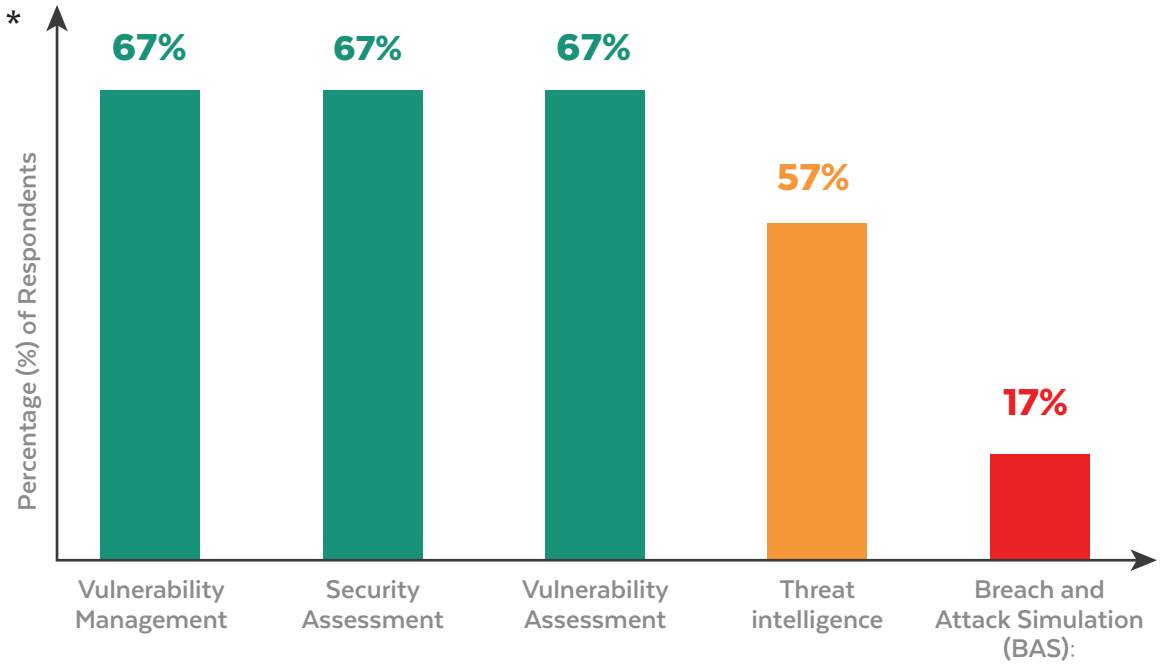
Key Takeaways

During the year, organizations faced several barriers in adequately defending against cyber threats. Findings from the survey include:

- Lack of security awareness among employees hindered 64% of respondents, emphasizing the need for comprehensive training to mitigate risks.
- 46% of respondents experienced a barrier due to a lack of skilled personnel, highlighting the importance of investing in cybersecurity talent acquisition and development.
- Budget constraints impacted 36% of respondents, limiting their ability to invest in strong security measures.
- 22% of respondents faced a barrier of lacking management support or awareness, emphasizing the significance of leadership involvement in the development a strong cybersecurity culture.

*Participants were allowed to select multiple options

What data protection technologies are already in use in your organization?



Key Takeaways

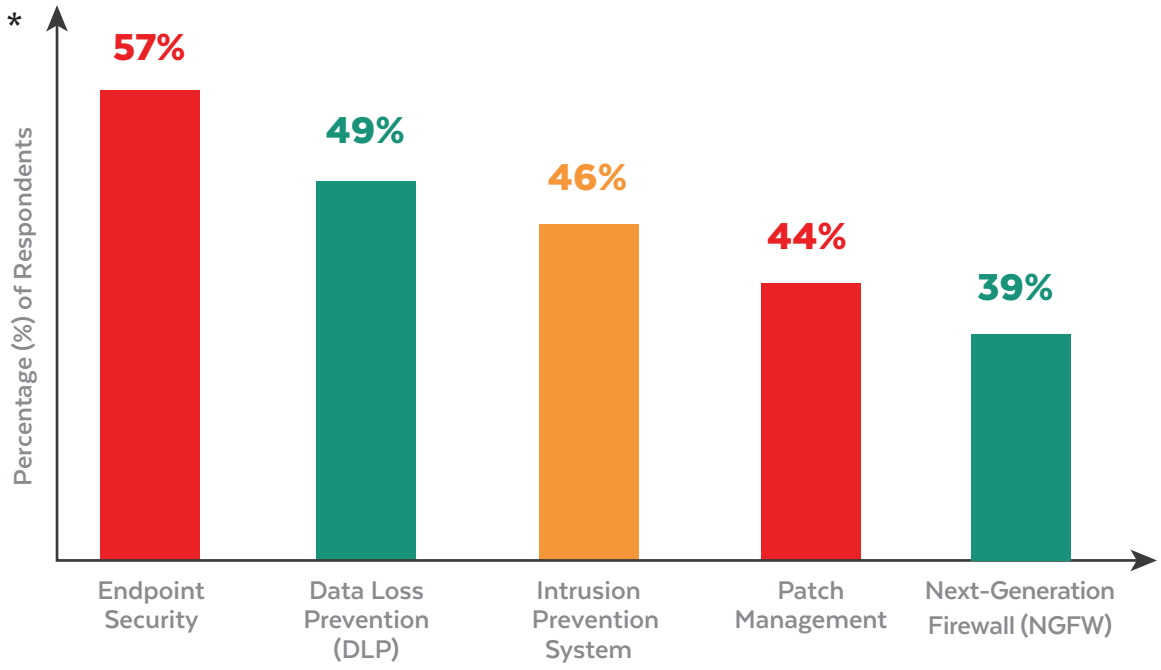
Organizations reported the use of various data protection technologies:

- **Vulnerability Management, Security Assessment, and Vulnerability Assessment:** These three data protection technologies are widely adopted, with each receiving 67% of respondents from iparticipants, ndicating their significance in organizational security strategies.
- **Threat Intelligence:** Close behind, Threat Intelligence received 57% of respondents highlighting its strategic importance in enabling organizations to proactively detect and respond to emerging threats.
- **Breach and Attack Simulation (BAS):** While the aforementioned technologies dominate the landscape, it's worth noting that Breach and Attack Simulation, with 17% of respondents votes, appears to be less commonly implemented. This indicates a potential area for growth or heightened awareness in the realm of data protection strategies.

Some organizations have not implemented any of the mentioned data protection technologies.

*Participants were allowed to select multiple options

What are the top 5 cyber threat prevention technologies that organizations should adopt?

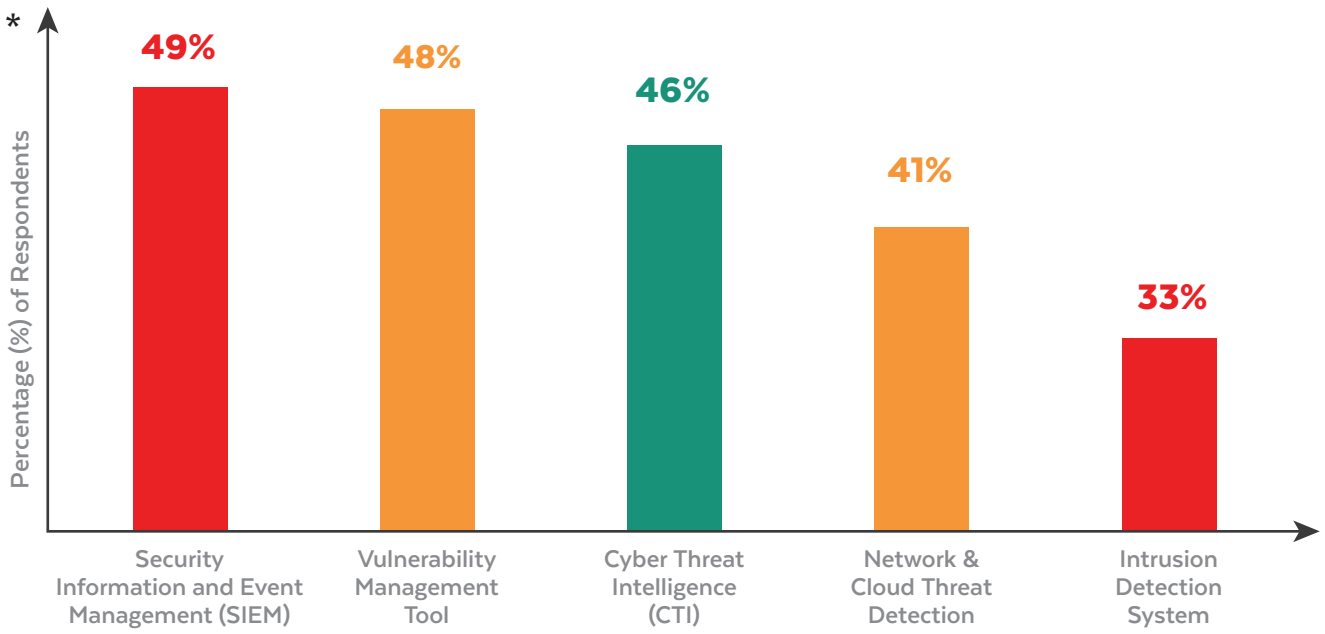


Key Takeaways

- **Endpoint Security:** A resounding 57% of respondents highlight the paramount importance of Endpoint Security in organizations' cyber threat prevention strategies.
- **Data Loss Prevention (DLP):** With 49% of respondents, Data Loss Prevention is also a high-priority area, securing sensitive information and intellectual property.
- **Intrusion Prevention System (IPS):** Intrusion Prevention System garnered 46% of respondents, underlining its importance in identifying suspicious activities and potential breaches.
- **Patch Management:** With 44% of respondents, Patch Management emerged as one of the top 5 cyber threat prevention technologies. It is integral in mitigating vulnerabilities that attackers may exploit.
- **Next-Generation Firewall (NGFW):** 39 percent of respondents recommended Next Generation Firewall (NGFW) as one of the top 5 essential controls

*Participants were allowed to select multiple options

What are the top 5 cyber threat detection technologies that organizations should adopt?



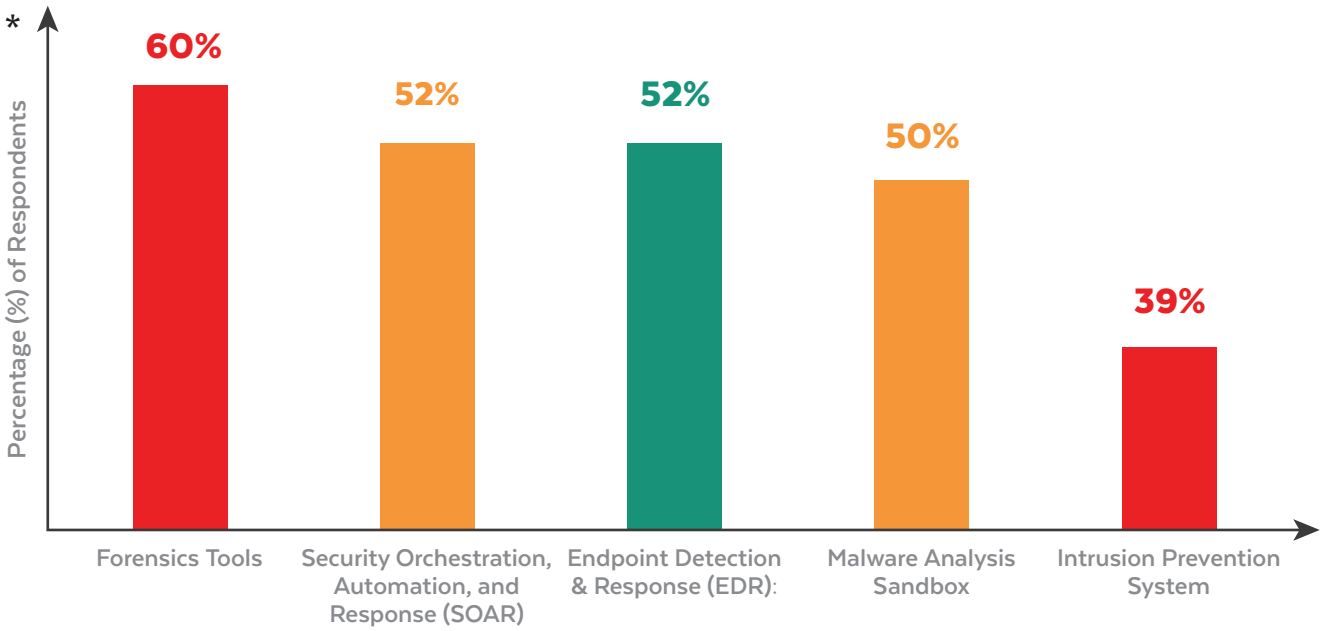
Key Takeaways

The top five cyber threat detection technologies that organizations identified as their current needs for adoption are as follows:

- **Security Information and Event Management (SIEM):** 49% of organizations recognized the importance of implementing SIEM solutions to effectively collect, analyze, and correlate security event data for enhanced threat detection.
- **Vulnerability Management Tool:** 48% of organizations expressed the need for vulnerability management tools to identify, prioritize, and remediate vulnerabilities in their systems and software.
- **Cyber Threat Intelligence (CTI):** 46% of organizations emphasized the adoption of CTI solutions to gather actionable insights about potential threats and enhance their threat detection capabilities.
- **Network & Cloud Threat Detection:** 41% of organizations recognized the significance of solutions focused on detecting threats within networks and cloud environments to protect against malicious activities and data breaches.
- **Intrusion Detection System:** 33% of organizations identified the adoption of intrusion detection systems as essential for detecting and responding to unauthorized access attempts and potential cyber threats.

*Participants were allowed to select multiple options

What are the top 5 cyber threat response technologies that organizations should adopt?



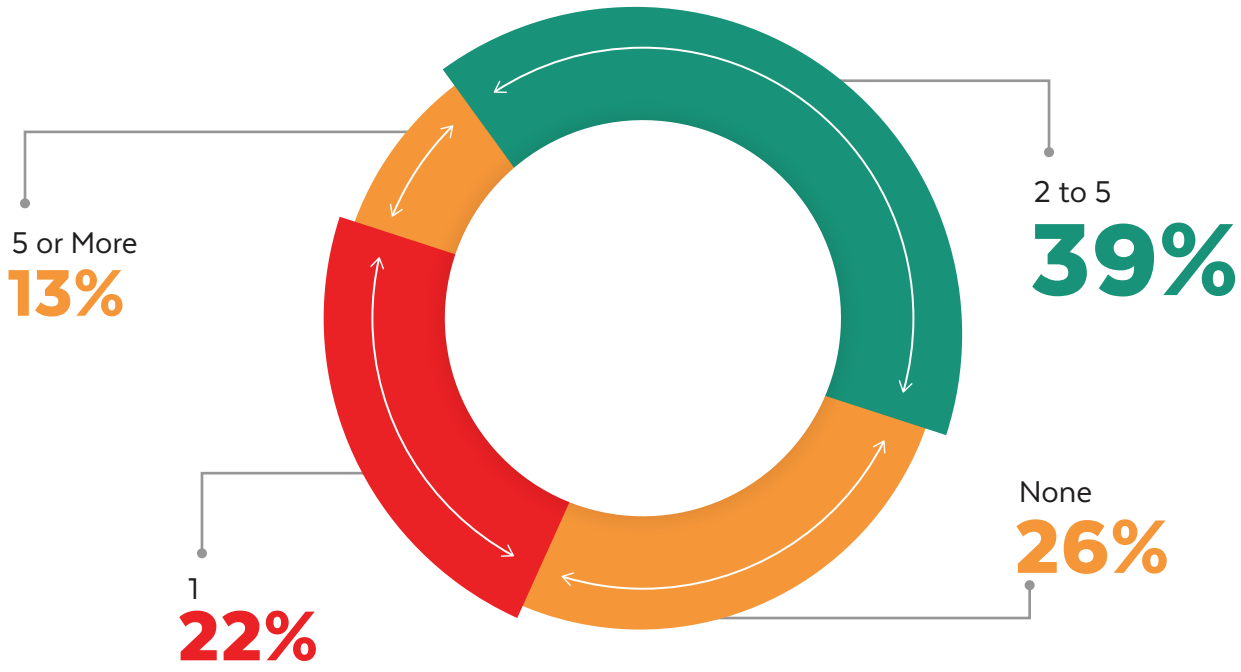
Key Takeaways

These findings underscore the importance of adopting these cyber threat response technologies to enhance incident response capabilities, automate processes, detect and analyze threats effectively, and strengthen defenses against cyber-attacks.

- **Forensics Tools:** 60% of respondents prioritize the adoption of forensics tools for investigating and analyzing cyber incidents, collecting evidence, and supporting incident response efforts.
- **Security Orchestration, Automation, and Response (SOAR):** 52% of respondents emphasize the importance of SOAR solutions to streamline and automate incident response processes, improving efficiency and effectiveness in mitigating threats.
- **Endpoint Detection and Response (EDR):** 52% of respondents consider EDR solutions as a priority for monitoring and detecting threats on endpoints, enabling rapid response and remediation.
- **Malware Analysis Sandbox:** 50% of respondents recognize the need for malware analysis sandbox tools to understand and analyze the behavior of malicious software, aiding in the development of effective response strategies.
- **Intrusion Prevention System:** 39% of respondents highlight the significance of intrusion prevention systems in proactively blocking and mitigating potential cyber threats, strengthening the organization's overall security posture.

*Participants were allowed to select multiple options

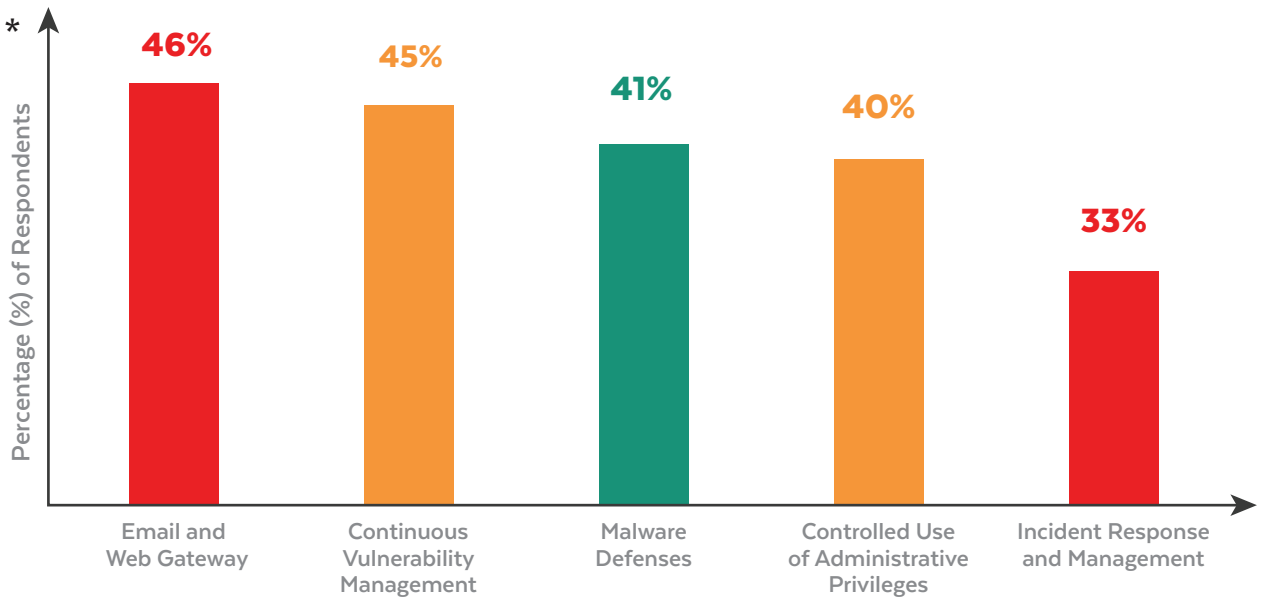
How many threat intelligence sources do you utilize as part of your threat detection and response programs?



Key Takeaways

These findings highlight the range of approaches organizations take in incorporating threat intelligence into their programs. While some organizations have yet to adopt any sources or rely on a single source, many recognize the value of multiple sources for a more comprehensive understanding of threats. By utilizing multiple threat intelligence sources, organizations can strengthen their ability to detect and respond to emerging cyber threats effectively.

The top five security controls that organizations found most effective during the year 2023 are as follows:



Key Takeaways

These findings underscore the importance of implementing these top five security controls to protect systems and data effectively. By focusing on email and web browser protections, continuous vulnerability management, robust malware defenses, controlled administrative privileges, and incident response capabilities, organizations can enhance their security posture and mitigate potential threats effectively.

- **Email and Web Gateway:** Effective email and web gateway play a vital role in mitigating security risks associated with email and web-based threats, as recognized by 46% of respondents.
- **Continuous Vulnerability Management:** Continuous management of vulnerabilities is essential for identifying and addressing potential security weaknesses promptly, according to 45% of respondents.
- **Malware Defenses:** Robust malware defenses are crucial for protecting against malicious software and preventing malware-related incidents, as highlighted by 41% of respondents.
- **Controlled Use of Administrative Privileges:** The controlled use of administrative privileges is effective in minimizing the risk of unauthorized access and potential misuse, as emphasized by 40% of respondents.
- **Incident Response and Management:** Having a well-defined incident response and management process in place is instrumental in effectively responding to and mitigating security incidents, as found by 33% of respondents.

*Participants were allowed to select multiple options

Does your organization provide employee training to raise information security awareness?

Key Takeaways

- 52% of respondents reported that their organization provides information security awareness training tailored to employees' job roles, indicating a proactive approach to equipping staff with essential security knowledge.
- Another 32% mentioned that their organization offers information security training but only occasionally, showing a commitment to periodically reinforcing security awareness.
- However, 16% of respondents stated that their organization does not provide information security awareness training, indicating a potential gap in security education that needs consideration.

Conclusion

Trillium Information Security Systems extends its sincere appreciation to all the organizations and individuals who participated in this survey. We are grateful for your continued support and engagement. Thank you, dear readers, for joining us once again on this journey. We genuinely hope that the information presented in this report has provided valuable assistance and that you found it both informative and easily comprehensible.

As highlighted throughout this year's report, the future can be unpredictable, and the path ahead may hold unforeseen challenges. However, by staying informed and connected, we can navigate these uncertainties more effectively. We strongly encourage you, our esteemed readers, to share your questions, comments, and thoughts with us. Your insights and perspectives contribute to a collective understanding and empower us to serve you better.

We strongly urge businesses to prioritize their cyber safety and take proactive measures in implementing resilient cybersecurity measures. By remaining vigilant and adopting a security-aware mindset, we can effectively protect ourselves and our organizations.